Communications of the Association for Information Systems

Volume 47 Article 4

10-11-2020

Understanding the Whistle-blowing Intention to Report Breach of Confidentiality

Wanyun Li
The Australian National University, wanyun.li@anu.edu.au

Ka Wai (Stanley) Choi
The Australian National University, stanley.choi@anu.edu.au

Shuk Ying Ho
Australian National University, susanna.ho@anu.edu.au

Recommended Citation

Li, W., Choi, K., & Ho, S. (2020). Understanding the Whistle-blowing Intention to Report Breach of Confidentiality. Communications of the Association for Information Systems, 47, pp-pp. https://doi.org/10.17705/1CAIS.04704

Communications of the Association for Information Systems

Research Paper DOI: 10.17705/1CAIS.04704 ISSN: 1529-3181

Understanding the Whistle-blowing Intention to Report Breach of Confidentiality

Wanyun Li
Research School of Accounting
The Australian National University
wanyun.li@anu.edu.au

Ka Wai (Stanley) Choi
Research School of Accounting
The Australian National University

Shuk Ying Ho
Research School of Accounting
The Australian National University

Abstract:

We examine the factors that encourage employees to whistle-blow wrongdoings in relation to confidentiality breaches. We investigate how their anticipated regret about remaining silent changes over time, how such changes influence their whistle-blowing intentions, and what employee characteristics and organizational policies moderate this relationship. Drawing on attribution theory, we develop three hypotheses. Our experiment findings show that: 1) employees' perceptions of the controllability and intentionality (but not stability) of the wrongdoing act affect how their anticipated regret evolves, 2) anticipated regret increases employees' whistle-blowing intentions, 3) anticipated regret has a stronger effect on whistle-blowing intentions when organizations implement policies that promote efforts to protect information confidentiality, and 4) employees with information technology knowledge have a stronger intention to whistle-blow. Theoretically, our study extends the organization security literature's focus to individuals' whistle-blowing and highlights an IS research agenda around whistle-blowing in relation to confidentiality breaches. Practically, it informs organizations about how to encourage employees to whistle-blow when they observe confidentiality breaches.

Keywords: Whistle-blowing, Attribution Theory, Organizational Policy, Confidentiality Breach.

This manuscript underwent peer review. It was received 04/14/2019 and was with the authors for seven months for two revisions. Indranil Bose served as Associate Editor.

1 Introduction

Digital information about individuals that organizations store has become increasingly complete and traceable, which has led to concerns about confidentiality breaches. Consequently, information systems (IS) researchers have invested substantial effort in increasing IS security to ensure the confidentiality, integrity, and availability of data that organizations hold in their systems (Boss, Galletta, Lowry, Moody, & Polak, 2015; Lowry, Moody, Galletta, & Vance, 2013; Posey, Roberts, & Lowry, 2015). Despite this effort, organizations may still experience security vulnerabilities, such as employees' inadvertently disclosing personal information and third parties' mishandling personal data (Debatin, Lovejoy, Horn, & Hughes, 2009; Iachello & Hong, 2007). Such vulnerabilities involve human beings, which means employees may learn about or notice such wrongdoings and potentially whistle-blow on them. In this paper, we examine the factors that lead employees to whistle-blow wrongdoings in relation to confidentiality breaches.

Whistle-blowing refers to an organization's former or current members' disclosing illegal, immoral, or illegitimate practices to persons or organizations that may be able to effect action (Near & Miceli, 1985). In general, researchers consider whistle-blowing an effective mechanism to uncover threats to public safety (Hwang, Staley, Te Chen, & Lan, 2008; Kaptein, 2011; Mesmer-Magnus & Viswesvaran, 2005; Taylor & Curtis, 2010; Vandekerckhove, 2018). However, thus far, researchers have examined whistle-blowing in relation to financial fraud. Even though IS researchers consider user information an asset as valuable as financial information (Posey, Roberts, Lowry, Bennett, & Courtney, 2013; Posey et al., 2015) and expect people to whistle-blow confidentiality breaches (Guo & Yu, 2019; Mamonov, Koufaris, & Benbunan-Fich, 2017; Padayachee, 2016; Posey et al., 2015; Tim, Pan, Bahri, & Fauzi, 2017; van Offenbeek, Boonstra, & Seo, 2017; Zhang & Leidner, 2018), they have not yet tested whether whistle-blowing applies to confidentiality breaches. We do not know whether whistle-blowing applies to confidentiality breaches because these breaches result in less obvious damage to organizations and even to victims; as such, employees may not consider reporting it necessary. To investigate this issue, we examine situational factors that that lead employees to whistle-blow wrongdoings related to confidentiality breaches. Accordingly, we propose our first research question (RQ):

> **RQ1:** What factors motivate employees to whistle-blow when encountering wrongdoings related to confidentiality breaches?

Although whistle-blowing reinforces a "speak-up" culture to protect employees and the public (Ciasullo, Cosimato, & Palumbo, 2017; Morrison & Milliken, 2000), employees often have psychological resistance to it. Specifically, whistle-blowers struggle between loyalty to their employer and a moral commitment to the law and society at large. Also, they often receive no support to protect them from retaliation (Buckley, Cotter, Hutchinson, & O'Leary, 2010; Kaplan & Schultz, 2007; Keil, Tiwana, Sainsbury, & Sneha, 2010; Mesmer-Magnus & Viswesvaran, 2005; Vandekerckhove, 2018). Whistle-blowing retaliation examples include demotion, social isolation, character assassination, and job loss (Keil et al., 2010; Mesmer-Magnus & Viswesvaran, 2005; Rehg, Miceli, Near, & Van Scotter, 2008; Vandekerckhove, 2018). As a result, whistle-blowers face a psychological battle in deciding whether to report a breach, but some experience anticipated regret about remaining silent. Regret refers to the emotion that decision makers feel when looking back at choices that went awry (Zeelenberg, Van Dijk, Manstead, & vanr de Pligt, 2000). But decision makers can also anticipate regret beforehand and consider it when evaluating different options as to avoid regret happening in the future (Fredin, 2011; Keil, Park, & Ramesh 2018). Investigating confidentiality breaches involves more complexity than investigating financial fraud because, unlike financial fraud, one cannot always accurately determine how much they cost their victims. Therefore, we argue that repeated confidentiality breaches will likely reduce employees' anticipated regret and increase their whistle-blowing intentions. Drawing on attribution theory, we identify three fraud-occurrence attributes (stability, controllability, and intentionality) and examine how they influence a potential whistle-blower's anticipated regret. Keil et al. (2018) examined potential whistle-blowers' anticipated regret with a cross-sectional view. Adding to Keil et al. (2018), we examine how their anticipated regret *evolves*. Accordingly, we propose:

> **RQ2:** When potential whistle-blowers have encountered multiple confidentiality breaches by their colleagues, how does their anticipated regret evolve over time?

Wrongdoings that concern confidentiality breaches can damage organizational reputation and place organizations under the risk of litigation (Ambrose & Gelb, 2001). IS researchers have examined the adverse impact that confidentiality breaches can have (e.g., Renaud, 2012; Smith, Dinev & Xu, 2011), such as negative public reactions to confidentiality breach announcements (e.g., Campbell, Gordon, Loeb

& Zhou; Kannan, Rees & Sridhar, 2007). Some IS researchers have proposed IS security measures (Bulgurcu, Cavusoglu, & Benbasat, 2010; Kankanhalli, Teo, Tan, & Wei, 2003; Siponen & Vance, 2010). However, few researchers have mentioned "whistle-blowing" specifically. As an exception, Lowry et al. (2013) proposed an online whistle-blowing reporting system in the workplace and identified key design features to promote whistle-blowing behaviors. In practice, however, many companies do not have the resources to establish an online whistle-blowing reporting system. Adding to prior research, we propose that organizations adopt whistle-blowing policies that urge potential whistle-blowers to voice their concerns when they detect wrongdoings. Implementing whistle-blowing policies presents a lower entry barrier to most companies than setting up an online whistle-blowing reporting system. Typical organizational practices include supervisor support (Mesmer-Magnus & Viswesvaran, 2005; Sims & Keenan, 1998), an ethical culture (Kaptein, 2011), an anonymous reporting channel (Kaplan & Schultz, 2007), and formal and informal whistle-blowing policies (Sims & Keenan, 1998). Research has found these organizational policies to effectively encourage whistle-blowing; however, such research has focused on only financial fraud. People may perceive confidentiality breaches to cause little damage, and thus, the aforementioned organizational policies may be less effective. In addition, individuals with limited technical knowledge can have difficulty understanding user information data mining and may be less likely to report confidentiality breaches. Accordingly, we propose:

RQ3: How do organizational policies and a potential whistle-blower's information technology (IT) knowledge promote whistle-blowing intentions?

We draw on attribution theory to develop three hypotheses. The hypotheses examine the relationship between the longitudinal change in anticipated regret and its subsequent effect on intention to whistle-blow. They also examine whether an employee's IT knowledge and the presence of organizational policies moderate the effect that anticipated regret has on whistle-blowing intentions. We conducted an online scenario-based experiment with 473 subjects who we tasked with reporting how they perceived wrongdoings related to confidentiality breaches in healthcare organizations. We ran a latent growth model (LGM) to analyze the data.

This paper proceeds as follows: in Section 2, we review the literature. In Section 3, we present attribution theory and develop the hypotheses. In Section 4, we present the experiment design. In Sections 5 and 6, we present and discuss our findings, respectively. Finally, in Section 7, we conclude the paper.

2 Background and Literature Review

In our study, confidentiality breaches involve personal information, such as an individual's health records, financial records, criminal records, political records, transaction records, business-related information, and Internet behavior (Hann, Hui, Lee, & Png, 2007; Langenderfer & Cook, 2004). Confidentiality breaches have drawn critical attention from the public partially due to the growing expectation that organizations will protect consumers' privacy. As the quantity of collected personal information continues to grow, people wish to maintain their anonymity and confidentiality (Debatin et al., 2009). Unfortunately, record digitization has increased the ease and speed with which organizations can share data with third parties and with which individuals can easily breach confidentiality. To detect confidentiality breaches, organizations in recent scandals on the Internet have relied on employees' whistle-blowing.

Whistle-blowing comprises six elements: 1) the disclosure of damaging news, 2) a whistle-blower agent, 3) a disclosure subject; 4) a target organization held responsible, 5) a disclosure recipient, and 6) a disclosure outcome (Mesmer-Magnus & Viswesvaran, 2005). Whistle-blowing can be internal or external depending on the disclosure recipient (Kaptein, 2011). Internal whistle-blowing involves reporting wrongdoings to a person outside the regular chain of command but in the organization, while external whistle-blowing involves reporting wrongdoings to an entity outside the organization, such as the media or a government agency, because the entity can stop or correct the wrongdoing. Among these two types of whistle-blowing, external whistle-blowing leads to severe consequences for the target organization held responsible such as public embarrassment, government scrutiny, hefty fines, or even litigation risks (Kaptein, 2011).

Although confidentiality breaches represent an important research topic, few studies have investigated whistle-blowing in relation to them. We reviewed papers published between 2009 and 2018 that concerned whistle-blowing (not specific to confidentiality breaches). We collected publications from six major IS journals: *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, *Journal of the Association for Information Systems*, *European Journal of Information Systems*,

and *Information Systems Journal*. We included three additional journals—*Decision Support Systems*, *Information and Management*, and *Communications of the Association for Information Systems*—because these journals publish papers on new and advanced developments in the IS discipline. Table 1 summarizes the literature we found.

Table 1. Publications that Mention "Whistle-Blowing"

Authors	Research objectives	Method	Findings and significance	Remarks
Guo & Yu (2019)	The authors examined the seemingly antithetical tension between discipline and anonymity in online settings. They highlighted how IT both enables and constrains how individuals balance the competing needs of anonymity and discipline.	Textual analysis on accountants' postings on an online forum.	The authors found that the online forum is an omniopticon in which the anonymous online self is disciplined and monitored in many ways. Information technology both enables and constrains how individuals balance the competing needs of anonymity and discipline.	While the authors did not focus on whistle-blowing, they mentioned that anonymity reduces psychological costs and can promote activities such as whistle-blowing.
Keil et al. (2018)	The authors focused on individuals' whistle-blowing intentions. In particular, the authors looked at health information privacy violations. They examined the role of attributions, the seriousness of wrongdoing, and emotion in shaping individuals' whistle-blowing intentions in the context of health information privacy violations.	Experiments of hypothetical scenarios to collect data.	The authors found that the seriousness of wrongdoing and people's emotion affect their whistle-blowing intentions.	Authors used whistle-blowing intention as a dependent variable.
Lee, Keil, Smith, & Sarkar (2017)	The authors focused on individuals' decision to report errors on IT projects. Specifically, they investigated the effects of mood (i.e., positive vs. negative) and a personality trait (conscientiousness) on error reporting decision.	A scenario-based laboratory experiment.	An individual's affective states and conscientiousness influence the individual's error reporting decisions. Further, mood moderates the relationship between conscientiousness and willingness to report.	Authors used intention to report errors as a dependent variable.
Lowry et al. (2013)	Whistle-blowing has long been a critical phenomenon that potentially places the firm and the whistle-blower at great risk. The paper explores the use of online whistle-blowing reporting systems in the workplace. The authors argue that anonymity, trust, and risk of online systems alter system usage. The authors propose a model specific to a whistle-blowing reporting system and examine the willingness to whistle-blow via the system, with the addition of trust, risk, and the multidimensional construct of anonymity.	An online experiment of hypothetical scenarios with working professionals.	The authors found that perceived risk of organizational failures and personal risk influence whistle-blowing behavior. The authors indicated that these nuanced conceptualizations and measures contribute important knowledge on whistle-blowing to both research and practice.	The authors used willingness to whistle-blowing as a dependent variable of the paper.

Table 1. Publications that Mention "Whistle-Blowing"

Mamonov et al. (2017)	Social networks leverage crowd-sourced information assets as essential pillars supporting their business models. However, the appropriation of rights to information assets through legal contracts often fails to prevent conflicts between the users and the companies that claim information rights. This paper examines why those conflicts arise and what their consequences are. The authors propose that intellectual property and privacy expectancies comprise core domains of psychological contracts between social networks and their users, and perceived breaches of those expectancies trigger a psychological contract violation. They use the exit, voice, loyalty, and neglect typology to define the user behavioral outcomes.	A cross-sectional survey of Facebook users to collect data and test hypotheses.	The authors found that perceived breaches to privacy and intellectual property rights generate the affective experience of a psychological contract violation, which is strongly associated with exit intentions.	The authors did not focus on whistle-blowing. However, they mentioned that the perceived breaches of privacy and intellectual property rights can possibly cause "voice" (of which whistle-blowing is an example).
Padayachee (2016)	The author focused on evaluating information security measures. To do so, the author drew on opportunity theories from the criminology discipline. The author evaluated extant opportunity-reducing techniques that organizations have employed to mitigate insider threats.	A three-round Delphi process with 23 experts from the industry.	The author conceptualized the element of opportunity in terms of the insider threat problem. Organizations can use this conceptualization to implement information security controls that should empower information security administrators to prevent and possibly counteract insider threats.	While the author did not focus on whistle-blowing, the author mentioned applicable techniques to overcome the insider threat problem and the increase in effort will likely promote whistle-blowing.
Posey et al. (2015)	The authors examined the role of organizational commitment in organization information security. Organizational commitment is a mechanism through which organizational security threats become personally relevant to insiders and how security education, training, and awareness efforts promote protective security behaviors.	A survey panel with insiders that a panel provider requisitioned.	The authors found that security education, training, and awareness efforts help insiders form appraisals. Also, they found that protection motivation theory also applies to organizational rather than personal contexts but that its applicability depends on insiders' organizational commitment levels. Through organizational commitment, organizational security threats become personally relevant to insiders and security education, training, and awareness efforts influence many components based on protection motivation.	While the authors did not focus on whistle-blowing, they mentioned whistle-blowing in the paper's practical implication section. They proposed strategies for avoiding retaliation and encouraging whistle-blowing.

Table 1. Publications that Mention "Whistle-Blowing"

Tim et al. (2017)	Digital technology is increasingly being recognized as a catalyst for national progress and social transformation. This paper explores the use of social media in bringing societal change through civic engagement. Taking a case study approach, the authors conceptualize how social media could be enacted to serve different boundary spanning purposes toward facilitating civic involvement.	An in-depth case study of social media-enabled crime-fighting communities in Malaysia.	Online users consider social media an important channel for whistle-blowing.	While the authors did not focus on whistle-blowing, but they mentioned it as a key role of social media to amplify citizen interest.
van Offenbeek et al. (2017)	The authors integrated two perspectives of technology adoption research: acceptance and resistance. They identified factors that lead to system acceptance and factors that lead to system avoidance.	Semi-structured telephone interviews from both urban and rural areas to capture users' intentions regarding system adoption.	The authors identified ambivalent reactions. In their sample, they found many users that support but do not use technology and others that resist but use technology. Their findings support the view that non-acceptance and resistance conceptually differ.	While the authors did not focus on whistle-blowing, they mentioned that whistle-blowing is an example of system resistance.
Zhang & Leidner (2018)	The authors focused on workplace cyberbullying. They examined how workplace cyberbullies justify their bullying behaviors and how cyber-communication features influence workplace cyberbullying behaviors.	A survey with employees across various job positions, companies, and industries to collect data and test hypotheses.	The authors found three denial-neutralization techniques (i.e., denial of injury, denial of responsibility, and denial of victim) that perpetrators use to justify their workplace cyberbullying behaviors and demonstrated the moderating effects of cyber communication features.	While the authors did not focus on whistle-blowing, they used the theory of neutralization and mentioned that neutralization exerts an effect on individuals' whistle-blowing intentions.

According to Table 1, IS researchers consider "whistle-blowing" a valid approach to address information security problems, but they have not focused on "whistle-blowing" specifically in their papers. Needless to say, we found even fewer papers that have examined employees' whistle-blowing specific to confidentiality breaches. We identified two exceptions: Keil et al. (2018) and Ciasullo et al. (2017). Keil et al. (2018) examined how confidentiality breach attributions influence employees' emotions in shaping their intention to whistle-blow to external parties. They examined how the intentionality and seriousness of health information privacy violations influence employees' anticipated regret about remaining silent and, subsequently, influence their willingness to report. Ciasullo et al. (2017) focused on organizational barriers and suggested that whistle-blowing requires an ethical culture and available anonymous reporting channels in an organization in relation to confidentiality breaches.

Based on the review we present above, we integrate Keil et al.'s (2018) psychological perspective and Ciasullo et al.'s (2017) management perspective to examine how employees' anticipated regret about not whistle-blowing changes over time. Inspired by recent scandals on the Internet, we consider whistle-blowers as employees in an organization. In March, 2018, attackers leaked more than 50 million Facebook user profiles to controversial political data analytics provider Cambridge Analytica, which might have helped Donald Trump win the 2016 presidential campaign. Facebook reviewed whether one of its own research employees knew about the leak. In March, 2011, HealthNet announced a confidentiality breach that affected two million of its insurance customers, which exposed their names, addresses, social security numbers, and health and financial data. The data, which lacked any encryption, resided in hard drives that the company found missing from the data center of its contractor, IBM. Individual employees caused these scandals, and outsiders or even management did not detect them. Therefore, protecting information confidentiality depends on employees' whistle-blowing.

3 Theory and Hypotheses Development

3.1 Attribution Theory

Attribution theory, a cognitive psychology theory, states that people attempt to understand others' behavior by attributing feelings, beliefs, and intentions to them. Individuals go through three steps to form an attribution (Griffin, 1991; Weiner, 1972): 1) observe an individual's behavior; 2) interpret the individual's behavior, attribute possible causes for it, and form emotional reactions according to those attributions; and 3) judge the individual. We apply this three-step process to whistle-blowing as follows: an employee observes an act of wrongdoing and assesses the wrongdoer's situation and then attributes observed misbehavior's possible causes to the wrongdoer to form an emotional reaction. These reactions subsequently affect the employee's intention to whistle-blow (Gundlach, Douglas, & Martinko, 2003).

The second stage deserves more attention because the way people interpret wrongdoing behavior's possible causes ultimately influences their whistle-blowing intention in regard to wrongdoers. Thus, we elaborate on the second step further. People interpret a behavior to attribute possible causes to the behavior. This attribution has three dimensions: locus of causality, stability, and controllability (Weiner, 1986). Locus of causality refers to the extent to which a behavior's cause originates internally or externally from the person (Harvey, Martinko, & Borkowski, 2017; Iglesias, Varela-Neira, & Vázquez-Casielles, 2015; Varela-Neira, Vázquez-Casielles, & Iglesias, 2014). With an internal locus of causality, actors can influence events and their behavior. In contrast, with an external locus of causality, situational forces drive actors' behaviors. Stability refers to the extent to which the observed behavior's causes remain unchanged over time. The causes can be permanent or transitory (Harvey et al., 2017; Keil et al., 2018; Thompson & O'Sullivan, 2017). Controllability refers to the extent to which one can manage a behavior's cause (Harvey et al., 2017; Iglesias et al., 2015; Thompson & O'Sullivan, 2017). With high controllability, people believe that they can avoid the wrongdoing if the wrongdoer behaves properly. In contrast, with low controllability, people do not accuse the wrongdoer of negligence but place blame on circumstances beyond the wrongdoer's control. In addition to the three dimensions that Weiner (1986) has identified, recent studies included one more dimension—intentionality (Harvey et al., 2017; Iglesias et al., 2015; Thompson & O'Sullivan, 2017). Intentionality refers to the extent to which people attribute a behavior's cause to purposive actions. People can commit wrongdoings purposefully or unintentionally.

In this study, we focus on stability, controllability, and intentionality. We do not consider locus of causality because, in the whistle-blowing context, an employee constitutes the individual who unethically uses personal information, and the typical external causality in the workplace—management's pressure on this employee—falls outside our research problem's scope because we examine data that an employee leaks without management's awareness.

3.2 Hypotheses Development

Drawing on attribution theory, we examine the effect that employees' psychological and organizational factors have on how employees' anticipated regret about not whistle-blowing changes over time and how organizational policies and employees' IT knowledge moderate the relationship between anticipated regret and intentions to whistle-blow. We present our research model in Figure 1.

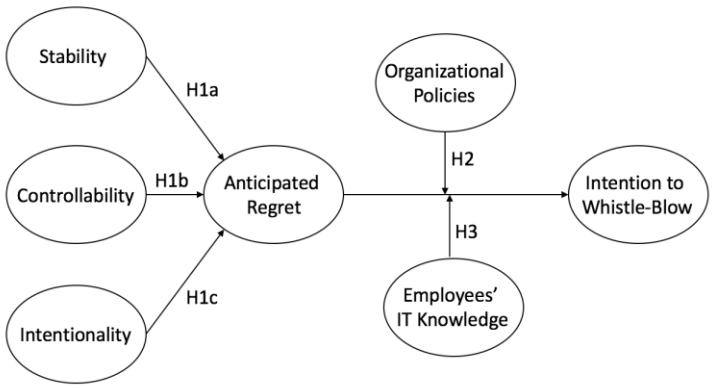

Figure 1. Research Model

3.2.1 Effect that Stability, Controllability, and Intentionality have on How Anticipated Regret about Remaining Silent Changes over Time

Drawing on attribution theory, we argue that, when employees discover a colleague engaging in confidentiality breach activities, they try to understand why the colleague performed this act and attribute the colleague's feelings, beliefs, and intentions to the organization (Griffin, 1991; Weiner, 1972). Prior studies have confirmed that the stability, controllability, and intentionality of the act that a wrongdoer performs elicit individuals to judge the wrongdoer's responsibility (Gundlach, Martinko, & Douglas, 2008; Harvey et al., 2017; Orsingher, Hogreve, & Ordanini, 2016). Specifically, when an employee finds a colleague who conducts the same wrongdoings for the same reasons (stability), to not volitionally alter wrongdoings even when they can (controllability) or to intentionally engage in wrongdoings (intentionality), then the employee will perceive the colleagues as responsible for their wrongdoings. Observers form moral emotions and guilt if they realize the present situation would have improved if they had made a choice other than remaining silent (Keil et al., 2018; King, 2001; Sandberg, Hutter, Richetin, & Conner, 2016). As a result, they anticipate regret. Prior studies have empirically proved the direct effect that perceived stability, controllability, and intentionality of a wrongdoing act have on regret (such as Sander & Scherer, 2009; Harrison-Walker, 2012). Adding to these studies, we examine how the three attributions (stability, controllability, and intentionality) affect how anticipated regret changes over time.

Interestingly, the intensity of anticipated regret changes over time. In other words, an interplay between inaction and time exists (Gilovich & Medvec, 1995; Itzkin, Van Dijk, & Azar, 2016; Towers, Williams, Hill, Philipp, & Flett, 2016). An employee's decision not to whistle-blow exemplifies inaction. In the following, we elaborate why anticipated regret grows in intensity with perceptions of wrongdoings' stability, controllability, and intentionality.

First, regret about inaction naturally grows over time (Gilovich & Medvec, 1995; Itzkin et al., 2016; Towers et al., 2016). When people decide not to act, they can have an inability to conquer their fears or hesitations when the "moment of truth" arrives (Abraham & Sheeran, 2003; Fredin, 2011; Keil et al., 2018). Employees choose not to inform their supervisors about a possible fraudulent act by a colleague because they lack certainty about the outcome. Employees strongly experience these negative emotions when making a decision, which can subsequently result in their inaction (Lerner, Li, Valdesolo, & Kassam, 2015); however, after these emotions fade, people begin to consider their inaction's consequences. A major reason why people anticipate regret about their inaction involves the possible good outcomes that would have arisen if they acted. Some people may even exaggerate the possible positive outcomes of acting (Gilovich & Medvec, 1995; Itzkin et al., 2016; Towers et al., 2016). As a result, their anticipated regret can magnify over time.

Second, when people collect more evidence that contradicts their decision to not act, their anticipated regret builds further. In our context, the more frequently employees observe a wrongdoing, the more confident they become in how they judge its stability, controllability, and intentionality. Wrongdoings that continue to occur do so because an employee did not take action in the past and act as a reminder to urge the employee to recall the inaction (Abraham & Sheeran, 2003; Miceli & Near, 2002; Rajagopal, Raju, & Unnava, 2006). When an employee views a colleague repeatedly commit a wrongdoing related to confidentiality breaches, the employee attributes a higher degree of 1) stability, 2) controllability, and 3) intentionality to the wrongdoing act, which causes the employee's anticipated regret to increase over time. Taken together, we predict that, when an employee observes a colleague commit wrongdoings more frequently, the employee anticipates more regret from remaining silent. Thus, we hypothesize:

H1: When an employee views a colleague repeatedly commit a wrongdoing related to confidentiality breaches, the employee's perceptions about its a) stability, b) controllability, and c) intentionality cause the employee's anticipated regret to increase over time

3.2.2 Moderation Effect that Employees' Information Technology Knowledge Has on the Relationship between Anticipated Regret and Intention to Whistle-Blow

One cannot easily determine whether anticipated regret about remaining silent triggers an employee to whistle-blow because, apart from whistle-blowing, employees have other options to stay away from wrongdoings. For instance, they may choose to tolerate the action, remain passive and silent, or even leave their organization (Hoffmann, 2006; Kaptein, 2002). We argue that, when an employee understands more about the potential harm that a confidentiality breach can cause to the public, then the employee will be more likely to whistle-blow. Using the 2018 Facebook scandal as an example, if an employee thinks

that businesses use Facebook data only to generate marketing advertisements, then the employee may choose to tolerate the act and have a low intention to whistle-blow. Conversely, if the employee realizes that political consultants can use Facebook data to bias presidential campaigns, then the employee may be more likely to whistle-blow.

We also need to consider which factors lead employees to better understand the potential harm that confidentiality breaches cause to the public. One such factor includes employees' IT knowledge. Analyzing user information to obtain actionable business knowledge involves sophisticated technical skillsets, such as data mining and analytics. Many recent scandals have involved big data (e.g., Cambridge Analytica scandal involved social media data, the Apple iPhone scandal involved location data, and the HealthNet scandal involved customer records), which is characterized by high volume, high data-generation speeds, and a variety of unstructured data formats. Data mining and big data analytics involve using high-end technology and complex computer algorithms to transform data into actionable business knowledge.

To elaborate, data mining involves extracting useful knowledge from digital data and sifting through it to identify information useful for prediction (Khan, Qureshi, & Hussain, 2014). Generally speaking, data mining relates to data warehouses (a large data store accumulated from various big data sources), cloud computing (a network of remote servers hosted on the Internet to store and process data), distributed computing (a network of high-performance computers for parallel processing), and deep learning and neural networks (a class of machine-learning methods based on learning data representations and nonlinear transformation for making predictions). Further, many companies merge multiple data types (such as location data and customer transactions) to deduce people's identities even when they deal with anonymous data (Bond-Graham, 2013; Ohm, 2012).

We argue that the outcomes that organizations can accomplish with data mining and big data analytics can be difficult for laypeople to understand. Thus, employees who do not know what data mining and big data analytics involve may underestimate problems that confidentiality breaches can pose to the public. These employees may think that data mining leads only to annoying online advertising or, at most, allows organizations to identify individuals' embarrassing information (Xu, Jiang, Wang, Yuan, & Ren, 2014). As a result, although they feel regret if something bad occurs, they lack confidence in how they judge wrongdoings associated with confidentiality breaches and, subsequently, have a low intention to whistle-blow.

In contrast, employees with IT knowledge can better understand why a company mines transactional data, how it merges multiple data sources to create a profile for individuals, and how it uses these profiles to understand their preferences and manipulate their future behavior. Therefore, these employees can more precisely assess data mining's potential risks to the public. Combined with anticipated regret as a trigger, they will be more likely to take action to minimize the threat from data mining and big data analytics to society than employees with low IT knowledge. Thus, we hypothesize:

H2: Anticipated regret about remaining silent exerts a stronger effect on intentions to whistle-blow for employees with high IT knowledge compared to employees with low IT knowledge.

3.2.3 Moderation Effect that Organizational Policies Have on the Relationship between Anticipated Regret and Intention to Whistle-Blow

We next examine how organizations can more proactively encourage employees to act when they discover confidentiality breaches in the workplace. For instance, organizations can consider establishing organization policies that outline information confidentiality protection acts and regulations in relation to handling individuals' personal data. Such policies articulate the importance of information confidentiality and instruct employees to deal with tasks in daily operations or to respond to requirements to comply with legislation, regulation, and codes of practice (Kohnke, Sigler, & Shoemaker, 2016). In brief, these policies communicate management's behavioral expectations about information protection to employees. We argue that the presence of these policies in an organization strengthen the relationship between anticipated regret and whistle-blowing intentions for three reasons, which we discuss below.

First, organizational policies in relation to information confidentiality help employees understand that any confidentiality breach constitutes a risk to the organization and even a threat to the public. Organizational policies also outline the crucial role that every employee needs to play in protecting information confidentiality. Moreover, the policies inform employees about how the organization supports them in handling confidentiality breaches (Doherty & Fulford, 2006; Maynard, Ruighaver, & Ahmad, 2011). As a

result, when organizations establish policies in relation to information confidentiality, employees better know their rights and responsibilities. Thus, when they witness their colleagues commit wrongdoings, they will be likely to whistle-blow.

Second, by establishing organizational policies in relation to confidentiality breaches, an organization signals its values to its employees. Organizational values comprise the organization's thoughts, beliefs, and actions. When employees do not know the organizational values, they may experience value conflicts. In our research context, when employees do not know the extent to which the organization values information confidentiality, they do not know if they should follow personal ethics or organizational norms in handling confidentiality breach (Erwin & Moncrieff, 2008; Smith, 1993). Employees may struggle to reconcile their personal concerns with the organizational norms and try to resolve these dilemmas by subjugating their personal beliefs to the organizational norms (Erwin & Moncrieff, 2008; Smith, 1993). Thus, by establishing organizational policies, organizations can signal to employees to maintain their personal ethical standards to act on confidentiality breaches in the workplace.

Third, organizational policies enable employees to understand their choices and opportunities when they witness confidentiality breaches. When employees witness wrongdoings, they may initially choose to remain silent. This "inaction" decision remains in their mind. Organizational policies inform employees about the options they possess to alter their prior inaction decision. The more employees reevaluate their prior inaction, the more they feel that they can act differently to alter the "mistakes" that their prior inaction caused and the stronger their desire to correct the prior inaction (Gilovich & Medvec, 1995), which promotes their intentions to whistle-blow. Thus, we hypothesize:

H3: Employees' anticipated regret about remaining silent exerts a stronger effect on their intentions to whistle-blow when their organization has organizational policies about maintaining information credibility compared to when their organization does not.

4 Method

4.1 Pretest

We followed Keil et al. (2018) to employ experiments with hypothetical scenarios to seek individuals' opinions about whistle-blowing. Before the main experiment, we recruited 28 university students to participate in a pretest. On average, it took them 20 minutes to complete the entire experiment. All students reported that they could easily understand the scenarios we used, but students without any work experience had some difficulty in understanding work ethics. Inspired by their comments, we interviewed six students with different levels of work experience to learn about how they understood work ethics. We found that students with a few months' work experience could elaborate their thoughts about work ethics well. Thus, in the main experiment, we recruited individuals who had at least three months' work experience.

4.2 Sample

In contrast to Keil et al. (2018), who adopted a laboratory experiment, we conducted an online experiment that we promoted via social media. By doing so, we could reach more potential subjects. According to the results from the pretests, we sought participants who had at least three months' work experience. We considered these people an appropriate target because they understood workplace ethics. Respondents could begin the online experiment at any time and place. In total, 612 respondents started the online experiment, and we collected 473 usable data points. Further, 329 participants were females and 144 were males. The average age was 25. Of the 473 respondents, 361 (76%) had more than 18 months' work experience.

Nonresponse bias, which can occur when respondents differ from nonrespondents, posed a concern for our study. To assess nonresponse biases, we compared the means for the demographics and major variables for early and late respondents. Other statistical tests, including demographic profiles and major variables in the model, were not significant. The only significantly different variable was age—early respondents tended to be younger than late respondents ($p < 0.1$)—an unsurprising result because young people tend to actively use social media and, thus, respond earlier.

4.3 Experiment Procedures

After the respondents began the experiment, we asked them to provide basic information about their demographics and work experience. Following this, we presented them with a case about a drug company that mined patients' healthcare records. We show this case, which we based on Keil et al. (2018)'s case with two modifications, in Appendix A. The first modification involved replacing HIPAA with the Privacy and Personal Information Protection Act 1998 in Australia because we recruited subjects in Australia. The second modification involved the number of scenarios we presented to subjects. Keil et al. (2018) examined the cross-sectional effect that that attributions have on anticipated regret; thus, they offered one scenario to each subject. In contrast, we examined the longitudinal change in anticipated regret. Thus, in our experiment, we presented three scenarios with the same company to describe a situation in which a colleague mined patients' healthcare records over time. After viewing each occasion, the subjects reported their opinions on the confidentiality breach, their anticipated regret, and their whistle-blowing intentions. At the end, we asked some open-ended questions to collect feedback from the subjects. The experiment took about 20 minutes.

4.4 Design and Measures

We did not manipulate the subjects' IT knowledge. Instead, we asked them to self-report their knowledge about 11 concepts related to data mining on a nine-point Likert scale (1 = "not knowledgeable about" to 9 = "very knowledgeable about") and computed the first score (i.e., the average of these 11 questions). We also asked them two open-ended questions about Web clickstream analysis and location tracking. Two researchers independently assessed their answers to assign the second score, which had nine marks in total. To measure subjects' IT knowledge, we averaged the two scores.

We manipulated the presence of organizational policies in the drug company through involving two groups in the experiment. We told the first group (the "with-policy" group) that the drug company had policies to encourage employees with ethical concerns to discuss them internally before proceeding to whistle-blow externally in order to create an overall environment in which employees had the opportunity and desire to behave ethically and responsibly. We also described the Australian Privacy and Personal Information Protection Act 1998 to the first group. We did not provide the second group (the "without-policy" group) any information about organizational policies or describe the Privacy and Personal Information Protection Act 1998.

We did not employ a full-factorial experiment design to test the effects that stability, controllability, and intentionality had on the anticipated regret about remaining silent because we did not intend to test their interactions. We followed Keil et al. (2018) to present scenarios with variations in company's wrongdoing's stability, controllability, and intentionality and allowed the subjects to freely form their own perceptions about the company's wrongdoing. We asked the subjects to self-report their perceptions. In doing so, we would find variance in how the subjects perceived stability, controllability, and intentionality. We present the instruments we used in our experiments in Appendix B. We present the descriptive statistics of our key variables in Table 2.

Table 2. Descriptive Statistics and Correlations

Variable	Mean (SD)		Correlation					
	Group 1	Group 2	A1	B1	C1	X1	X2	X3
A1	3.96 (1.18)	1.96 (0.83)	1					
B1	3.29 (1.18)	1.65 (0.90)	0.03	1				
C1	5.00 (1.65)	4.45 (2.85)	0.51**	0.10*	1			
X1	4.25 (0.81)	2.02 (1.16)	0.45**	0.10*	0.50**	1		
X2	6.04 (0.80)	5.67 (2.31)	0.02	0.31**	0.16**	0.42**	1	
X3	6.90 (1.35)	7.16 (2.27)	-0.09	-0.11*	-0.04	0.30**	0.34**	1
W3	7.84 (1.19)	4.05 (2.20)	0.42**	0.04	0.53**	0.82**	0.45**	0.45**

Notes: A1 = stability at t1; B1 = controllability at t1; C1 = intentionality at t1; X1 = anticipated regret at t1; W3 = whistle-blowing intentions at t3. ** $p < 0.01$, * $p < 0.05$.

4.5 Latent Growth Model Approach

We conducted LGM analysis using AMOS 17.0 to test our three hypotheses. LGM, a statistical technique for analyzing longitudinal data, emphasizes the change in trajectory in the outcome variable over time (Duncan et al., 1994) (in our case, anticipated regret's trajectory). LGM analysis suits efforts to analyze changes in behavior when one has an a priori hypothesis about changes in trajectory over time (i.e., slope) (Duncan, Duncan, & Stoolmiller, 1994), which H1 focused on.

LGM created a regression-type line for the outcome variable (anticipated regret) for each person over time (Byrne, 2016). We estimated two latent factors: one that represented the subject's baseline anticipated regret (the intercept) and one that represented changes in anticipated regret over time (the slope). These factors corresponded to the distinctions we define in Section 3 between initiation and change in the dependent variables of interest. To represent individuals' baseline level of anticipated regret, we created the intercept factor with a fixed loading of 1.0 at each wave. To represent individuals' changing anticipated regret over time, we created the slope factor with a fixed loading of 0.0 at T1 and, thereby, established the other factor as the intercept. We assumed strict linearity in the slope factor in which case we would fix the slope loadings to 0.0, 0.5, and 1.0 to represent three equally spaced measurement occasions (Byrne, 2016). The perceptual variables at T1 (stability, controllability, and intentionality) were the predictor variables of primary interest. All predictors in the model were from T1 so that the predictive relations would be prospective. We used individuals' anticipated regret at T1, T2, and T3 to predict their intention to whistle-blow. Following Keil et al. (2018), we controlled for the effect that demographic variables (age, gender, work experience, and personal risk of reporting the failure) had on individuals' intention to whistle-blow.

We separated our LGM analysis for the two groups we used in the experiment. For the without-policy group, we ran LGM analysis with 224 data points. The mean intercept of anticipated regret was 1.41, which corresponds to the mean of anticipated regret (2.02) at T1. The mean slope was 5.04. Both the mean intercept and the mean slope were significantly greater than zero ($p < 0.01$). For the with-policy group, we ran LGM analysis with 249 data points. The mean intercept of anticipated regret was 3.59, which corresponds roughly to the mean of anticipated regret (4.23) at T1. The mean slope was 3.47. A positive mean slope concurs with an increase in anticipated regret over time. Both the mean intercept and the mean slope were significantly greater than zero ($p < 0.01$). Taking the two groups together, organizational policies promoted a higher starting value of anticipated regret at T1 ($3.59 > 1.41$), but a smaller slope of anticipated regret (from T1 to T3) ($3.47 < 5.04$) over time.

5 Hypotheses Testing

5.1 Hypothesis 1

H1 posits that, when an employee views a colleague repeatedly commit a wrongdoing related to confidentiality breaches, the employee's perceptions about its a) stability, b) controllability, and c) intentionality cause the employee's anticipated regret to increase over time. To test it, we first ran LGM analysis with 249 data points from the with-policy group. We found that perceived stability of a wrongdoer's act did not have any effect on the slope of anticipated regret (estimate = -0.08, $p > 0.1$) or on its intercept (estimate = 0.06, $p > 0.1$). Thus, we did not find support for H1a. Next, we found that perceived controllability exerted a positive effect on the starting point of anticipated regret (estimate = 0.18, $p < 0.01$) and its slope (estimate = 0.25, $p < 0.01$). Thus, we found support for H1B. Finally, we found that perceived intentionality exerted a positive effect on the slope of anticipated regret (estimate = 0.18, $p < 0.1$). Thus, we found marginal support for H1c.

We then analyzed 224 data points from the without-policy group. We found that perceived stability of a wrongdoer's act did not have any effect on the slope of anticipated regret (estimate = 0.10, $p > 0.1$). Thus, we did not find support for H1a. However, we found that perceived stability exerted an effect on the starting point of anticipated regret (estimate = 0.27, $p < 0.01$). This finding indicates that the subject's perceived stability did not affect the change in trajectory in anticipated regret but did affect its starting value. Next, we found that perceived controllability exerted a positive effect on the slope of anticipated regret (estimate = 0.09, $p < 0.01$). Thus, we found support for H1b. Finally, we found that perceived intentionality exerted a positive effect on the slope of anticipated regret (estimate = 0.29, $p < 0.01$). Thus, we found support for H1c.

Taking the analyses together, we found that a subject's perceived controllability and intentionality affected how anticipated regret changed over time, yet perceived stability influenced the starting point of anticipated regret but not its slope. Our findings imply that, regardless of whether an organization has implemented organizational policies, the way people perceive a wrongdoing's controllability and intentionality (but not stability) affect how anticipated regret changes over time. Perceived stability's nonsignificant effect probably resulted due to the nature of digital data. To elaborate, to commit financial fraud, an employee may make multiple transactions to transfer money out from an organization's account to avoid attracting attention. Stability indicates a wrongdoing's severity. In contrast, one can easily copy and transfer digital data, and one could potentially transfer millions of transactions with a mouse click. Therefore, people may not need to observe multiple data transfers to confirm such a wrongdoing's severity.

5.2 Hypotheses 2 and 3

H2 posits that anticipated regret about remaining silent exerts a stronger effect on intentions to whistle-blow for employees with high IT knowledge compared to employees with low IT knowledge. We merged our two datasets and used 473 data points to run a regression with whistle-blowing intentions as the dependent variable to test this hypothesis. The independent variables included the average of anticipated regret across the three time points, employees' IT knowledge, organizational policies, and their interactions. We controlled for the effect that age, gender, work experience, and fear of retaliation had on whistle-blowing intentions. Fear of retaliation exerted a negative effect (estimate = -0.21, $p < 0.01$) on whistle-blowing intentions. Females had a weaker intention than males ($p < 0.05$). Age and work experience did not exert any significant effect on whistle-blowing intentions.

We found that the interaction between employees' IT knowledge and anticipated regret was nonsignificant for whistle-blowing intentions (estimate = -0.46, $p > 0.1$). Thus, we did not find support for H2. However, we found that IT knowledge had a significant positive main effect on whistle-blowing intentions (estimate = 2.45, $p < 0.05$). The positive estimate suggests that employees with high IT knowledge tend to form a stronger intention to whistle-blow when they see colleagues commit a wrongdoing than do employees with low IT knowledge. We undertook a median split to divide the 473 data points into high IT knowledge and low IT knowledge groups. The mean of whistle-blowing intentions of the group with high IT knowledge was 6.59, and the mean of the group with low IT knowledge was 5.09. We found a significant difference between the two means ($t = 6.58$, $p < 0.01$).

We then examined the presence of organizational policies. The interaction between the presence of organizational policies and anticipated regret exerted a significant effect (estimate = 0.65, $p < 0.01$) on whistle-blowing intentions. The positive estimate suggests that organizational policy promotes a stronger intention to whistle-blow when employees see wrongdoings. The mean whistle-blowing intention of the with-policy group was 7.84, and the mean of the without-policy group was 4.05. We found a significant difference between the two means ($t = 23.64$, $p < 0.01$). Hence, we found support for H3. Table 3 summarizes our findings.

Table 3. Summary of Main Findings

Hypothesis	Result
H1a: When an employee views a colleague repeatedly commit a wrongdoing related to confidentiality breaches, the employee's perceptions about its stability cause the employee's anticipated regret to increase over time.	Not supported
H1b: When an employee views a colleague repeatedly commit a wrongdoing related to confidentiality breaches, the employee's perceptions about its controllability cause the employee's anticipated regret to increase over time.	Supported
H1c: When an employee views a colleague repeatedly commit a wrongdoing related to confidentiality breaches, the employee's perceptions about its intentionality cause the employee's anticipated regret to increase over time.	Supported
H2: Anticipated regret about remaining silent exerts a stronger effect on their intentions to whistle-blow for employees with high IT knowledge compared to employees with low IT knowledge.	Supported
H3: Employees' anticipated regret about remaining silent exerts a stronger effect on their intentions to whistle-blow when their organization has organizational policies about maintaining information credibility compared to when their organization does not.	Supported

6 Discussion

6.1 Theoretical and Practical Contributions

With this study, we contribute to the organization security literature by extending its focus to individuals' whistle-blowing. Given that organizations have widely adopted IS and electronic commerce, they digitalize data to enhance their operations and make intelligent decisions (Debatin et al., 2009; Iachello & Hong, 2007; Sutlieff & Chelin, 2010). However, such practices raise concerns about information confidentiality. These practices may lead to not only inadvertent disclosure of personal information but also damaged reputation, unwanted harassment, hacking, and identity theft (Debatin et al., 2009; Iachello & Hong, 2007). Information confidentiality represents an ethical and legal problem for the public (Debatin et al., 2009; Iachello & Hong, 2007). Inspired by recent scandals in which employees leaked user data to third parties, we examine ways to promote whistle-blowing when an individual observes confidentiality breaches by their colleagues in the workplace. In particular, our study contributes to theory and practice in three ways.

First, our study confirms that employees care about information confidentiality. When employees notice confidentiality breaches, they become alert, and some regret if they choose to remain silent. These findings align with the literature on whistle-blowing in relation to financial fraud (Kaplan & Schultz, 2007). Adding to the literature, our study indicates that, when employees see confidentiality breaches, their anticipated regret increases over time, although some employees do not take immediate action for various reasons (e.g., some may suffer a conflict between loyalty to the organization and loyalty to a wider constituency, and some may be worried about retaliation). This finding represents good news for organizations and society—people understand that confidentiality breaches are unethical and possibly illegal and have a sense of responsibility to protect information confidentiality. Our study extends the organization security literature's focus to individuals' whistle-blowing and highlights an IS research agenda around whistle-blowing in relation to confidentiality breaches.

Second, our study indicates that people with high IT knowledge are more likely to report wrongdoings, and people with low IT knowledge may regret remaining silent but lack confidence in their judgment and choose not to whistle-blow. Without IT training, even if employees know about ethical principles and information confidentiality, they lack the knowledge to detect individual employees who leak information to third parties. Thus, their poor judgment leads to lower whistle-blowing intentions and a failure to report confidentiality breaches. Therefore, to promote employees' intentions to protect information confidentiality, organizations should provide both work ethics workshops and IT training related to information confidentiality. IT training could focus on big data analytics in commercial applications and information handling in data centers and warehouses. For example, since 2016, the Bank of New York Mellon Corporation, a global banking and finance company, has offered data analytics training to its employees and integrated this training into their commercial applications (Wang, 2016). Since early 2018, National Australia Bank (NAB, 2018), one of the largest banks in Australia, has started providing a cloud skills training program to employees to handle digital data. Given the digital era, organizations should provide IT training to all staff to increase their awareness of data leaks and confidentiality breaches.

Third, our study confirms that organization policies can promote whistle-blowing intentions. Despite organizations' efforts to increase data security, management may not know that individual employees have leaked data to third parties. To minimize this risk, organizations can establish policies to inform all employees about organizational values and provide support to whistle-blowers. Further, we suggest that governments place more emphasis on the importance of information confidentiality. Governments already allocate resources for fraud-control arrangements. For instance, in the United States, the SEC Enforcement Division's Financial Reporting and Audit Group identifies and prosecutes securities law violations related to financial reporting and audit failures. Governments invest relatively less resources in preventing, detecting, and dealing with information confidentiality. For example, in the United States, the Federal Trade Commission regulates laws to protect consumers' privacy (O'Conner, 2018). However, no single federal regulation mandates organizations to establish an information confidentiality policy; rather, the country focuses on industry self-regulation (O'Conner, 2018). Europe has taken the lead on privacy policy. The European Union implemented the General Data Protection Law (GDPR) from 25 May, 2018 (Ashford, 2018; Yu, 2018). This law protects individual personal information and applies to all organizations that deal with the data of European Union citizens (Ashford, 2018; Yu, 2018). The GDPR mandates that organizations, such as Facebook, must ask for consent from users before they collect their personal information. Organizations also need to explain in detail why they need users' information and how they use it (Ashford 2018; Yu 2018). The data that the GDPR covers include credit numbers, travel

records, religious affiliations, Web search results, biometric data from wearable fitness monitors, and Internet protocol addresses (Ashford, 2018; Yu, 2018). Although the GDPR represents a big step toward information confidentiality, it remains inadequate on its own. For example, many organizations have developed artificial intelligence algorithms to analyze people's behavior on social media and mobile apps, which the GDPR does not cover and intellectual property rights protect (Ashford, 2018; Yu, 2018). Information confidentiality certainly constitutes a complex issue to which governments must devote increased attention. Collaborative efforts between governments and organizations can prevent individual employees leaking organizational data to third parties.

6.2 Limitations and Future Research

Our study has several limitations. First, we recruited our subjects online through social media. Although recruiting subjects online meant we could extend and diversify our sample, these subjects generally hold stronger computer knowledge than individuals who have never used social media. Their stronger computer knowledge might have caused a favorable effect on understanding the severity of digital information infringements. Second, individuals' ethical standards that guide their whistle-blowing behaviors may depend on culture, which we do not consider in our study. Thus, we encourage future research to explore how culture is associated with anticipated regret and whistle-blowing intentions. Third, we used healthcare as the experiment context to study confidentiality breaches. In general, people are sensitive to confidentiality breaches in relation to health information. Future research could explore whether our research model applies to examine other types of confidentiality breaches, such as transaction records, location trails, and personal emails.

7 Conclusions

In this paper, we focus on wrongdoings related to confidentiality breaches and examine how wrongdoing attributions affect the trajectory of anticipated regret and whistle-blowing intentions. We draw on attribution theory to develop three hypotheses and test them with data that we collected in an experiment. Our findings indicate that how employees perceive a wrongdoing's controllability and intentionality (but not stability) affect how their anticipated regret about remaining silent changes over time (H1). In addition, high IT knowledge (H2) and the presence of organizational policies (H3) promote whistle-blowing intentions. With this paper, we contribute to the literature by highlighting how whistle-blowers' anticipated regret about remaining silent changes over time. In addition, we pinpoint the challenge of encouraging employees who have observed wrongdoings to take action. We suggest two approaches to address this challenge: 1) equip employees with strong IT knowledge to handle sensitive data and 2) establish organizational policies on information confidentiality. These actionable suggestions can help organizations reinforce professionalism and ethical behavior in relation to handling confidential data in the workplace.

Acknowledgments

We thank the Editor in Chief, the Associate Editor, and the two reviewers for their valuable feedback.

References

Abraham, C., & Sheeran, P. (2003). Acting on intentions: The role of anticipated regret. *British Journal of Social Psychology, 42*(4), 495-511.

Ambrose, S. F., Jr., & Gelb, J. W. (2001). Consumer privacy regulation and litigation: The business lawyer. Chicago, *56*(3), 1157-1178.

Ashford, W. (2018). New UK data protection act not welcomed by all. *ComputerWeekly*. Retrieved from https://www.computerweekly.com/news/252441814/New-UK-Data-Protection-Act-not-welcomed-by-all

Bond-Graham, D. (2013). Iron cagebook. *Counterpunch*. Retrieved from https://www.counterpunch.org/2013/12/03/iron-cagebook/

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837-864.

Buckley, C., Cotter, D., Hutchinson, M., & O'Leary, C. (2010). Empirical evidence of lack of significant support for whistleblowing. *Corporate Ownership and Control, 7*(3), 275-283.

Bulgurcu, B., Cavusoglu, H., & Benbasast, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

Byrne, B. M. (2016). *Structural equation modeling with AMOS: Basic concepts, applications, and programming*. New York, NY: Routledge.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431-448.

Ciasullo, M. V., Cosimato, S., & Palumbo, R. (2017). Improving health care quality: The implementation of whistleblowing. *The TQM Journal, 29*(1), 167-183.

Culiberg, B., & Mihelič, K. K. (2017). The evolution of whistleblowing studies: A critical review and research agenda. *Journal of Business Ethics, 146*(4), 787-803.

Danis, M., Farrar, A., Grady, C., Taylor, C., O'Donnell, P., Soeken, K., & Ulrich, C. (2008). Does fear of retaliation deter requests for ethics consultation? *Medicine, Health Care and Philosophy, 11*(1), 27-34.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security, 25*(1), 55-63.

Duncan, T. E., Duncan, S. C., & Stoolmiller, M. (1994). Modeling developmental processes using latent growth structural equation methodology. *Applied Psychological Measurement*, *18*(4), 343-354.

Erwin, G., & Moncrieff, M. (2008). Investing in online privacy policy for small business as part of B2C web site management: Issues and challenges In K. Klinger, K. Rosh, J. Neidig & J. Snavely (Eds.), *Information communication technologies: Concepts, methodologies, tools, and applications* (pp. 2998-3006). New York, NY: IGI Global.

Fredin, A. J. (2011). The effects of anticipated regret on the whistleblowing decision. *Ethics & Behavior, 21*(5), 404-427.

Gilovich, T., & Medvec, V. H. (1995). The experience of regret: What, when, and why. *Psychological Review, 102*(2), 379-395.

Griffin, E. (1991). Attribution theory of Firitz Heider In S. Gouijinstook & T.Z. Ackley (Eds.), *A first look at communication theory* (pp. 137-145). New York, NY: McGraw-Hill.

Gundlach, M. J., Douglas, S. C., & Martinko, M. J. (2003). The decision to blow the whistle: A social information processing framework. *Academy of Management Review, 28*(1), 107-123.

Gundlach, M. J., Martinko, M. J., & Douglas, S. C. (2008). A new approach to examining whistle-blowing: The influence of cognitions and anger. *SAM Advanced Management Journal, 73*(4), 40-50.

Guo, K. H., & Yu, X. (2019). The anonymous online self: Toward an understanding of the tension between discipline and online anonymity. *Information Systems Journal*, *30*(1), 48-69.

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24*(2), 13-42.

Harrison-Walker, L. J. (2012). The role of cause and affect in service failure. *Journal of Services Marketing, 26*(2), 115-123.

Harvey, P., Martinko, M. J., & Borkowski, N. (2017). Justifying deviant behavior: The role of attributions and moral emotions. *Journal of Business Ethics, 141*(4), 779-795.

Hoffmann, E. A. (2006). Exit and voice: Organizational loyalty and dispute resolution strategies. *Social Forces, 84*(4), 2313-2330.

Hwang, D., Staley, B., Te Chen, Y., & Lan, J.-S. (2008). Confucian culture and whistle-blowing by professional accountants: An exploratory study. *Managerial Auditing Journal, 23*(5), 504-526.

Iachello, G., & Hong, J. (2007). End-user privacy in human-computer interaction. *Foundations and Trends in human–computer interaction, 1*(1), 1-137.

Iglesias, V., Varela-Neira, C., & Vázquez-Casielles, R. (2015). Why didn't it work out? The effects of attributions on the efficacy of recovery strategies. *Journal of Service Theory and Practice, 25*(6), 700-724.

Imhoff, R., Wohl, M. J., & Erb, H. P. (2013). When the past is far from dead: How ongoing consequences of genocides committed by the ingroup impact collective guilt. *Journal of Social Issues, 69*(1), 74-91.

Itzkin, A., Van Dijk, D., & Azar, O. H. (2016). At least I tried: The relationship between regulatory focus and regret following action vs. inaction. *Frontiers in Psychology, 7*, 1-16.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce, 12*(1), 69-91.

Kaplan, S. E., & Schultz, J. J. (2007). Intentions to report questionable acts: An examination of the influence of anonymous reporting channel, internal audit quality, and setting. *Journal of Business Ethics, 71*(2), 109-124.

Kaptein, M. (2002). Guidelines for the development of an ethics safety net. *Journal of Business Ethics, 41*(3), 217-234.

Kaptein, M. (2011). From inaction to external whistleblowing: The influence of the ethical culture of organizations on employee responses to observed wrongdoing. *Journal of Business Ethics, 98*(3), 513-530.

Keil, M., Park, E. H., & Ramesh, B. (2018). Violations of health information privacy: The role of attributions and anticipated regret in shaping whistle-blowing intentions. *Information Systems Journal, 28*(5), 818-848.

Keil, M., Tiwana, A., Sainsbury, R., & Sneha, S. (2010). Toward a theory of whistleblowing intentions: A benefit-to-cost differential perspective. *Decision Sciences, 41*(4), 787-812.

Khan, A., Qureshi, M. S., & Hussain, A. (2014). Improved genetic algorithm approach for sensitive association rules hiding. *World Applied Sciences Journal, 31*(12), 2087-2092.

King, G. (2001). Perceptions of intentional wrongdoing and peer reporting behavior among registered nurses. *Journal of Business Ethics, 34*(1), 1-13.

Kohnke, A., Sigler, K., & Shoemaker, D. (2016). *The complete guide to cybersecurity risks and controls*. Boca Raton, FL: CRC Press.

Langenderfer, J., & Cook, D. L. (2004). Oh, what a tangled web we weave: The state of privacy protection in the information economy and recommendations for governance. *Journal of Business Research, 57*(7), 734-747.

Lee, H. K., Keil, M., Smith, H. J., & Sarkar, S. (2017). The roles of mood and conscientiousness in reporting of self-committed errors on IT projects. *Information Systems Journal*, *27*(5), 589-617.

Lerner, J. S., Li, Y., Valdesolo, P., & Kassam, K. S. (2015). Emotion and decision making. *Annual Review of Psychology, 66*, 799-823.

Lowry, P. B., Moody, G. D., Galletta, D. F., & Vance, A. (2013). The drivers in the use of online whistle-blowing reporting systems. *Journal of Management Information Systems*, *30*(1), 153-190.

Mamonov, S., Koufaris, M., & Benbunan-Fich, R. (2017). The role of user psychological contracts in the sustainability of social networks. *Communications of the Association for Information Systems*, *40*, 218-248.

Maynard, S., Ruighaver, A., & Ahmad, A. (2011). Stakeholders in security policy development. In *Proceedings of the 9th Australian Information Security Management Conference*.

Mesmer-Magnus, J. R., & Viswesvaran, C. (2005). Whistleblowing in organizations: An examination of correlates of whistleblowing intentions, actions, and retaliation. *Journal of Business Ethics, 62*(3), 277-297.

Miceli, M. P., & Near, J. P. (1984). The relationships among beliefs, organizational position, and whistle-blowing status: A discriminant analysis. *Academy of Management Journal, 27*(4), 687-705.

Miceli, M. P., & Near, J. P. (1985). Characteristics of organizational climate and perceived wrongdoing associated with whistle-blowing decisions. *Personnel Psychology, 38*(3), 525-544.

Miceli, M. P., & Near, J. P. (1992). *Blowing the whistle: The organizational and legal implications for companies and employees*. New York, NY: Lexington Books.

Miceli, M. P., & Near, J. P. (2002). What makes whistle-blowers effective? Three field studies. *Human Relations, 55*(4), 455-479.

Morrison, E. W., & Milliken, F. J. (2000). Organizational silence: A barrier to change and development in a pluralistic world. *Academy of Management Review, 25*(4), 706-725.

NAB. (2018). *NAB lauches Cloud Guild to develop AWS skills.* Retrieved from https://news.nab.com.au/news_room_posts/nab-launches-cloud-guild-to-develop-aws-skills/#resources

Near, J. P., & Miceli, M. P. (1985). Organizational dissidence: The case of whistle-blowing. *Journal of Business Ethics & Behavior, 4*, 1-4.

O'Conner, N. (2018). Reforming the U.S. approach to data protection and privacy. *Council on Foreign Relations*. Retrieved from https://www.cfr.org/report/reforming-us-approach-data-protection

Ohm, P. (2012). Don't build a database of ruin. *Harvard Business Review*. Retrieved from https://hbr.org/2012/08/dont-build-a-database-of-ruin

Orsingher, C., Hogreve, J., & Ordanini, A. (2016). Building on the past: Advancing theory in services through meta-analysis. *Journal of Service Management, 27*(1), 37-42.

Padayachee, K. (2016). An assessment of opportunity-reducing techniques in information security: An insider threat perspective. *Decision Support Systems*, *92*, 47-56.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS* Quarterly, *37*(4), 1189-1210.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214.

Rajagopal, P., Raju, S., & Unnava, H. R. (2006). Differences in the cognitive accessibility of action and inaction regrets. *Journal of Experimental Social Psychology, 42*(3), 302-313.

Rehg, M. T., Miceli, M. P., Near, J. P., & Van Scotter, J. R. (2008). Antecedents and outcomes of retaliation against whistleblowers: Gender differences and power relationships. *Organization Science, 19*(2), 221-240.

Renaud, K. (2012). Blaming noncompliance is too convenient: What really causes information breaches? *IEEE Security & Privacy*, *10*(3), 57-63.

Sandberg, T., Hutter, R., Richetin, J., & Conner, M. (2016). Testing the role of action and inaction anticipated regret on intentions and behaviour. *British Journal of Social Psychology, 55*(3), 407-425.

Sander, D., & Scherer, K. (2009). *Oxford companion to emotion and the affective sciences.* Oxford, UK: Oxford University Press.

Sims, R. L., & Keenan, J. P. (1998). Predictors of external whistleblowing: Organizational and intrapersonal variables. *Journal of Business Ethics, 17*(4), 411-421.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487-502.

Smith, H. J. (1993). Privacy policies and practices: Inside the organizational maze. *Communications of the ACM, 36*(12), 104-122.

Smith, J. H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989-1016.

Sutlieff, L., & Chelin, J. (2010). “An absolute prerequisite”: The importance of user privacy and trust in maintaining academic freedom at the library. *Journal of Librarianship and Information Science, 42*(3), 163-177.

Taylor, E. Z., & Curtis, M. B. (2010). An examination of the layers of workplace influences in ethical judgments: Whistleblowing likelihood and perseverance in public accounting. *Journal of Business Ethics, 93*(1), 21-37.

Thompson, A. E., & O’Sullivan, L. F. (2017). Understanding variations in judgments of infidelity: An application of attribution theory. *Basic and Applied Social Psychology, 39*(5), 262-276.

Tim, Y., Pan, S. L., Bahri, S., & Fauzi, A. (2017). Digitally enabled crime-fighting communities: Harnessing the boundary spanning competence of social media for civic engagement. *Information & Management*, *54*(2), 177-188.

Towers, A., Williams, M. N., Hill, S. R., Philipp, M. C., & Flett, R. (2016). What makes for the most intense regrets? Comparing the effects of several theoretical predictors of regret intensity. *Frontiers in Psychology, 7*, 1-8.

Vandekerckhove, W. (2018). Whistleblowing and information ethics: Facilitation, entropy, and ecopoiesis. *Journal of Business Ethics, 152*(1), 15-25.

Van Offenbeek, M., Boonstra, A., & Seo, D. (2013). Towards integrating acceptance and resistance research: Evidence from a telecare case study. *European Journal of Information Systems*, *22*(4), 434-454.

Varela-Neira, C., Vázquez-Casielles, R., & Iglesias, V. (2014). Intentionality attributions and humiliation: The impact on customer behavior. *European Journal of Marketing, 48*(5/6), 901-923.

Wang, A. X. (2016). The future of staff training is getting employees to train themselves. *Quartz*. Retrieved from https://qz.com/770290/the-future-of-staff-training-is-getting-employees-to-train-themselves/

Weiner, B. (1972). Attribution theory, achievement motivation, and the educational process. *Review of Educational Research, 42*(2), 203-215.

Weiner, B. (1985). An attributional theory of achievement motivation and emotion. *Psychological Review, 92*(4), 548-573.

Weiner, B. (1986). Attribution, emotion, and action. In R. M. Sorrentino & E. T. Higgins (Eds.), *Handbook of motivation and cognition* (pp. 281-312). New York, NY: Guilford.

Wong, K. F. E., Yik, M., & Kwong, J. Y. (2006). Understanding the emotional aspects of escalation of commitment: The role of negative affect. *Journal of applied psychology, 91*(2), 282.

Xu, L., Jiang, C., Wang, J., Yuan, J., & Ren, Y. (2014). Information security in big data: Privacy and data mining. *IEEE Access, 2*, 1149-1176.

Yu, H. (2018). GDPR isn't enough to protect us in an age of smart algorithms. *The Conversation*. Retrieved from https://theconversation.com/gdpr-isnt-enough-to-protect-us-in-an-age-of-smart-algorithms-97389

Zeelenberg, M., Van Dijk, W. W., Manstead, A. S., & vanr de Pligt, J. (2000). On bad decisions and disconfirmed expectancies: The psychology of regret and disappointment. *Cognition & Emotion, 14*(4), 521-541.

Zhang, S., & Leidner, D. (2018). From improper to acceptable: How perpetrators neutralize workplace bullying behaviors in the cyber world. *Information & Management*, *55*(7), 850-865.

Appendix A: Experiment Scenarios

Scenario for Round 1

You work for a drug company that has developed a Web-based system for individuals to maintain their electronic health records. You have recently learned that your supervisor is mining the protected health information and using it to market the company's drug products. This use of protected health information violates the Privacy and Personal Information Protection Act (1998) and could cause financial, reputational, or other harm if the information falls into the wrong hands.

"In your company, all employees receive proper healthcare privacy training and should be aware that mining health records and using them for marketing purposes is in violation of the Privacy and Personal Information Protection Act (1998)." (Your supervisor is new to the healthcare industry and is completely unaware that mining health records and using them for marketing purposes is in violation of the Privacy and Personal Information Protection Act (1998).) "This is the first time your supervisor has illegally mined health records and used them for marketing purposes." (This is not the first time your supervisor has illegally mined health records and used them for marketing purposes.) "There is a prior contract that mandates your department to share the results of data mining of health records with the drug company." (There is no prior contract that mandates your department to share the results of data mining of health records with the drug company.)

Now, you are faced with the decision about whether to draw your supervisor's actions to the attention of others, such as the management of the company or even bodies outside the organization. If you decide to report your supervisor's actions, you could upset management and even lose your job. However, if you remain silent, one or more individuals could suffer financial, reputational, or other harm if their protected health information falls into the wrong hands.

Scenario for Round 2

You have recently learned that your supervisor is again mining protected health information and using it to market the company's drug products.

"By now, your supervisor should have received proper healthcare privacy training offered by your company and should be aware that the mining of health records and its use for marketing purposes is in violation of the Privacy and Personal Information Protection Act (1998)." (Without any healthcare privacy training, your supervisor is likely to be completely unaware that the mining of health records and using them for marketing purposes is in violation of the Privacy and Personal Information Protection Act (1998).) "This is the second time your supervisor has illegally mined health records and used them for marketing purposes." (You have witnessed a few times that your supervisor has illegally mined health records and used them for marketing purposes.) "There is a prior contract that mandates your department to share the results of data mining of health records with the drug company. This contract will expire in December 2019." (There is no prior contract that mandates your department to share the results of data mining of health records with the drug company.)

Now, you are faced with the decision about whether to draw your supervisor's actions to the attention of others, such as the management of the company or even bodies outside the organization. If you decide to report your supervisor's actions, you could upset management and even lose your job. However, if you remain silent, one or more individuals could suffer financial, reputational, or other harm if their protected health information falls into the wrong hands.

Scenario for Round 3

You have recently learned that your supervisor is again mining protected health information and using it to market the company's drug products.

"By now, your supervisor should be aware that the mining of health records and using them for marketing purposes is in violation of the Privacy and Personal Information Protection Act (1998)." (Without any healthcare privacy training, your supervisor may be completely unaware that the mining of health records and using them for marketing purposes is in violation of the Privacy and Personal Information Protection Act (1998).) "This is the third time your supervisor has illegally mined health records and used them for marketing purposes." (You have witnessed a few times that your supervisor has illegally mined health

records and used them for marketing purposes.) “There is a prior contract that mandates your department to share the results of data mining of health records with the drug company. This contract has been extended for one more year until the end of 2020.” (There is no prior contract that mandates your department to share the results of data mining of health records with the drug company.)

Now, you are faced with the decision about whether to draw your supervisor’s actions to the attention of others, such as the management of the company or even bodies outside the organization. If you decide to report your supervisor’s actions, you could upset management and even lose your job. However, if you remain silent, one or more individuals could suffer financial, reputational, or other harm if their protected health information falls into the wrong hands.

Appendix B: Survey Instruments

Whistle-blowing intention (Gundlach et al., 2003; Keil et al., 2010; Miceli & Near, 1984, 1985):

1) I intend to report my supervisor’s actions with respect to the Privacy and Personal Information Protection Act (1998) to the management of my company. (1 = definitely not; 9 = definitely)
2) I intend to report my supervisor’s actions with respect to the Privacy and Personal Information Protection Act (1998) to an external auditor. (1 = definitely not; 9 = definitely)
3) I intend to tell an outside authority, such as the Department of Human Services, about my supervisor’s actions with respect to the Privacy and Personal Information Protection Act (1998). (1 = definitely not; 9 = definitely)

Stability of wrongdoing (Gundlach et al., 2003; Keil et al., 2010; Weiner, 1985):

1) The illegal mining of health records was part of an ongoing pattern of behavior. (1 = definitely not; 9 = definitely)

Controllability of wrongdoing (Gundlach et al., 2003; Keil et al., 2010; Weiner, 1985):

1) The supervisor could have controlled the illegal mining of health records. (1 = definitely not; 9 = definitely)

Intentionality of wrongdoing (Gundlach et al., 2003; Keil et al., 2010; Weiner, 1985):

1) The supervisor intentionally violated the Privacy and Personal Information Protection Act (1998). (1 = definitely not; 9 = definitely)

Seriousness of wrongdoing (Gundlach et al., 2003; Keil et al., 2010; Miceli & Near, 1985, 1992):

1) How serious is the potential harm to individuals from the violations of the Privacy and Personal Information Protection Act (1998)? (1 = not at all; 9 = very much)
2) How much financial, reputational, or other harm could result from the use of protected health information for marketing purposes? (1 = not at all; 9 = very much)

Anticipated regret about remaining silent (Keil et al., 2010; Wong, Yik, & Kwong, 2006; Zeelenberg et al., 2000):

1) If you decided to remain silent about your supervisor’s action and then later learned that an individual’s confidential health records about their depression and suicide attempts were used to send free samples of an antidepressant to their work address, which caused the employee to lose their job, to what extent would you regret your decision to remain silent? (1 = no regret; 9 = very much regret)

Fear of retaliation (Danis et al., 2008):

1) I am worried that I may lose my job as a result of reporting unethical behaviors in the company. (1 = not at all; 9 = very much)
2) I am worried that I will experience retaliation as a result of reporting the unethical behaviors of senior employees. (1 = not at all; 9 = very much)

About the Authors

Wanyun Li is a PhD candidate in the Research School of Accounting at the Australian National University. She started her PhD in 2018. Her research interests focus on the impact of big data (including social media and news media) on accounting problems. She has published her work in *Accounting and Finance*.

Ka Wai (Stanley) Choi is Lecturer of Accounting at the Australian National University. His research interests cover financial accounting, disclosure regulations, capital markets and social media. He has published in a number of accounting and information systems journals.

Shuk Ying Ho is Professor of Information Systems at the Australian National University. Her research interests cover personalization, electronic government, open source software development, social media, data analytics, and accounting information systems. She has served or is serving on the editorial boards of *MIS Quarterly*, *Journal of the Association for Information Systems*, and *Communications of the Association for Information Systems*.